ABSTRACT

An Asynchronous Enhanced Shared Secret Provisioning Protocol (ESSPP) provides a novel method and system for adding devices to a network in a secure manner. A registration process is launched by at least one of two network devices together. These two devices then automatically register with each other. When two devices running Asynchronous ESSPP detect each other, they exchange identities and establish a key that can later be used by the devices to mutually authenticate each other and generate session encryption keys. An out-of-band examination of registration signatures generated at the two devices can be performed to help ensure that there was not a man-in-the-middle attacker involved in the key exchange.